UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
NORTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

Case Number 11-20219
Honorable Thomas L. Ludington

JAMES R. DRIVER,

Defendants.
_____/

OPINION AND ORDER GRANTING THE GOVERNMENT'S MOTION IN LIMINE TO INCLUDE EVIDENCE OF OTHER ACTS INEXTRICABLY INTERTWINED WITH THE CHARGED ACTS

On April 12, 2012, the Government filed a motion in limine to include evidence of other acts as inextricably intertwined with the charged acts and, alternatively, as proper evidence admissible under Federal Rule of Evidence 404(b). ECF No. 26. The Government subsequently filed an amended motion, explaining that it no longer seeks to introduce the testimony of Ben Hicks, and is thus no longer moving to admit his testimony under Rule 404(b). ECF No. 36. The Government now only seeks admission of testimony from the undercover agent that the Limewire Global Unique Identifier ("GUID") number used by the defendant in the charged dates matched the GUID number of an individual trading child pornography in Florida just a few months prior as a fact intrinsic to the case to explain the steps taken by the undercover agent to identify defendant, and not excludable under Rule 404 as improper character evidence.

The Court ordered Defendant to file an expedited response (ECF No. 28) and Defendant requested an extension of time to file a response, which was granted (ECF No. 39). Defendant's response was due on or before May 7, 2012. *Id.* As of today's date, no response has been filed. For the reasons provided herein, the Government's motion in limine will be granted.

I. Facts

Special Agent Kay Een ("SA Een"), Naval Criminal Investigative Service, began investigating Defendant James R. Driver, on September 4, 2008, from her location in San Diego, California. SA Een was conducting undercover operations on the Gnutella peer-to-peer network. Peer-to-peer networks allow users who install file sharing software to trade or exchange files directly between computers. There are several such networks, such as Gnutella, which is the network used in this case. File sharing programs like Limewire and Phex allow users to share files across the internet on the Gnutella network. A user on the network has the option of making files on his computer available for sharing. Users on some networks gain higher status if they share more files, which gives them priority and faster speeds when downloading files from other users. The Gnutella network also allows users to view shared files using the "Browse Host" option. Once the file sharing software has identified another user with the desired files, the searching user may use this command to see a list of all files on that host computer. The Browse Host command will also display the host user's IP address, as well as the filename and the hash value of available files. Files may only be seen in this manner if the user has made them available for sharing.

File sharing software like Limewire allows users to search the network for desired files by using search terms or hash values. A hash value is an alphanumeric algorithm that functions like a file's DNA or fingerprint - they are essentially unique, up to 99.99%. The name of a file can change, but the hash value remains the same as long as the content is unchanged. A user can also "dial up" another user by entering an Internet Protocol ("IP") address into the software and then connect over the network. An IP address is uniquely assigned at a given moment in time by a user's Internet Service Provider ("ISP"). On a peer-to-peer network, an IP address functions like a telephone

number, as it allows one user to connect to another and establishes an internet connection by which each user can download files from another.

An investigator may then use several publicly available resources to try and identify a network user. Any user on the network can see the IP address of another user. The agent can enter the IP address into one of several publicly available websites that identify which ISP owns a particular IP address. ISPs own a certain spectrum of IP addresses, which are then assigned to their subscribers. Once the ISP is identified, the agent may then send a subpoena to the ISP to find out which subscriber was assigned a particular IP address at a given time. ISPs are required to maintain this information for six months. Investigators may also use publicly available website services to geolocate an IP address, which will tell them the region where an ISP assigned a certain IP address. This allows investigators to target network users who are within their jurisdiction. Another technique is to use the GUID, which is a 32-character alphanumeric sequence that also operates to identify a given computer on the network. A GUID is uniquely assigned by the file sharing software program. Any user on the network can view the GUID of another user.

All of this information can be uploaded by the investigator onto the Wyoming IDN Toolkit, which is then stored on servers maintained by the State of Wyoming. The Wyoming IDN Toolkit was developed by the Wyoming Internet Crimes Against Children ("ICAC") Task Force to assist law enforcement officers with tracking, storing, and sharing their investigative activity as part of what it calls "Operation Fairplay." For example, an investigator using Limewire can search the Gnutella network using the search term "PTHC" (which represents the phrase "preteen hardcore") to identify users on the network who are offering files for download with PTHC in the filename. An investigator can upload the IP address, the date and time, the hash value, and the file name to the

Wyoming IDN Toolkit database. Other investigators using the Wyoming Toolkit can then research this database to see if a given IP address has been previously identified as potentially trading child pornography. This is often used by investigators to determine the value of a target to see whether further investigation is warranted.

The Wyoming ICAC Task Force also uses an automated software program called Peer Spectre to look for files using known search terms. This software tool captures the same information (IP address, date/time, hash value, filename) and automatically catalogues it on the database. This information is also available to other investigators. The database tracks who made the identification, either a particular investigator or Peer Spectre.

SA Een has been trained by the Wyoming ICAC Task Force on how to use the Wyoming IDN Toolkit to assist her investigations. SA Een began her investigation by using several of the techniques described above. SA Een first searched the Wyoming database for IP addresses that identified potential targets in or accompanying the United States Armed Forces. SA Een found an IP address that was owned by Americable International of Japan, which is a United States company based in Florida that provides cable and internet services to military personnel stationed in Japan. SA Een entered the IP address 61.213.185.91 into her file sharing software program and connected to Defendant's computer in Japan, where he was stationed with United States Navy. She executed the "Browse Host" command and retrieved a list of files that defendant had made available for sharing, the size, the hash value, the name of each, and that the defendant was using Limewire. She repeated this process on September 12 and September 19, 2008, and captured the file list on those occasions. The files names were indicative of child pornography, and the hash values had been identified by other Wyoming IDN Toolkit as suspected child pornography.

According to Americable records, this IP address was assigned during September 2008 to Petty Officer John Bardenhagen, USN, Yokuska, Japan, in Apartment 26, Jyuban Towers, which is an apartment building leased to the United States as a dormitory for naval personnel. Apartment 26 is a suite that houses four male naval servicemen. Naval housing records reflect that Bardenhagen moved out of the apartment on September 10, 2008. The same records reflect that Defendant moved into Apartment 26 between July 24 and August 12, 2008. On October 1, 2008, the Americable account was switched to Defendant's name, and he set up a shared internet connection for him and his three suitemates. When the account changed names, Americable assigned it a new IP address of 203.205.118.130.

SA Een found this new IP address by searching the Wyoming database as described above. She again browsed the files available for sharing on the Gnutella network from that IP address and referenced the Wyoming IDN Toolkit database. These checks revealed that the Limewire-assigned GUID for both the 61.213.185.91 and the 203.205.118.130 IP addresses was the same, suggesting a strong likelihood that this was the same computer. SA Een captured the file list from this second IP address five more times in October and November 2008, which again indicated suspected child pornography.

On January 22, 2009, SA Een reviewed the history of this GUID on the Wyoming database. This particular GUID had been flagged by the Peer Spectre program 53 times between March 20, 2008, and April 2, 2008, as having files available for download with names suggestive of child pornography. Furthermore, the GUID was associated during that time period with the IP address 68.200.93.204.

SA Een found that the IP address was owned at that time by Road Runner LLC, St.

Petersburg, Florida, and that it geolocated to nearby Palm Harbor, Florida. A review of Defendant's military records shows that he was stationed at Corry Station, Pensacola, Florida. Based on this information, SA Een and NCIS identified Driver as the primary suspect.

On January 23, 2009, Defendant was interviewed by NCIS agents. Defendant agreed to speak with them and admitted that he had been downloading pornography since he was 15 years old using Limewire and U-Torrent, another file sharing program.

II. Discussion

"Rule 404(b) does not extend to evidence of acts which are 'intrinsic' to the charged offense." 1991 Advisory Committee Note; *United States v. Barnes*, 49 F.3d 1144, 1149 (6th Cir. 1995); *United States v. Rozin*, 664 F.3d 1052 (6th Cir. 2012); *United States v. Marrero*, 651 F.3d 453, 471 (6th Cir. 2011) (citing *United States v. Henderson*, 626 F.3d 326, 338 (6th Cir. 2010)) (" '[w]here the challenged evidence is 'intrinsic' to, or 'inextricably intertwined' with evidence of, the crime charged, Rule 404(b) is not applicable' "). Intrinsic acts "are those that are part of a single criminal episode," *Barnes*, 49 F.3d at 1149, including evidence that is "inextricably intertwined with evidence of the crime charged," *United States v. Everett*, 270 F.3d 986, 992 (6th Cir. 2001) (citing *Barnes*, 49 F.3d at 1149), or "part of a continuing pattern of illegal activity." *Barnes*, 49 F.3d at 1149.

The Sixth Circuit has recognized the "propriety of introducing 'background' evidence." *United States v. Hardy*, 228 F.3d 745, 748 (6th Cir. 2000). As it is intrinsic to the charged offense, Rule 404(b) does not apply to background evidence, which "consists of those other acts that are inextricably intertwined with the charged offense or those acts, the telling of which is necessary to complete the story of the charged offense." *Id.*; *see also United States v. Clay*, 667 F.3d 689,

697-98(6th Cir. 2012); *United States v. Gonzalez*, 501 F.3d 630, 639 (6th Cir. 2007).

Proper background evidence has a causal, temporal or spatial connection with the charged offense. Typically, such evidence is a prelude to the charged offense, is directly probative of the charged offense, arises from the same events as the charged offense, forms an integral part of a witness's testimony, or completes the story of the charged offense. *Marrero*, 651 F.3d at 471 (citing *Hardy*, 228 F.3d at 748).

After identifying the IP address which was offering files indicative of child pornography, Agent Een subpoenaed the relevant internet service provider and discovered that the IP address led to a residence which housed four male naval servicemen. In order to determine which of the four individuals was offering the files indicative of child pornography for download, Agen Een reviewed the history of the Limewire assigned GUID which was offering files indicative of child pornography to be downloaded.

The Government notes that a review of the history showed that this particular GUID had been flagged by the Peer Spectre program 53 times between March 20, 2008, and April 2, 2008, as having files available for download with names suggestive of child pornography. Furthermore, the GUID was associated during that time period with the IP address 68.200.93.204. SA Een found that the IP address was owned at that time by Road Runner LLC, St. Petersburg, Florida, and that it geolocated to nearby Palm Harbor, Florida. A review of Defendant's military records shows that he was stationed at Corry Station, Pensacola, Florida. Based on this information, SA Een and NCIS identified Defendant as the primary suspect among the four individuals associated with the IP address.

Such type of evidence is "inextricably intertwined with the charged offense" and "is

necessary to complete the story of the charged offense" and should be admitted. *United States v. Frederick*, 406 F.3d 754, 761 (6th Cir. 2005) (citation omitted) (recognizing background evidence as an"exception to the prohibitions of Rule 404(b)"). The Government asserts that excluding this evidence would only serve to mislead the jury with an incomplete version of events. "Proper background evidence has a causal, temporal, or spatial connection with the charged offense." *Id.* (quotations and citations omitted). In *United States v. Rhodes*, 314 F. App'x 790, 793 (6th Cir. 2008) (unpublished), the Sixth Circuit held that "evidence of the controlled purchase and drugs found at the apartment," which were not charged offenses, were inextricably intertwined with the firearms charges because the evidence "explain[ed] why the police raided [the] apartment." Similarly, SA Een's discovery that the same GUID involved in offering images of child pornography were offering images in Florida just immediately prior to the charged time period explains why the investigators identified Defendant as the prime suspect and should be admitted as proper background or identification evidence.

Based on the facts presented by the Government, Agent Een's testimony that the Limewire GUID number used by Defendant in the charged dates matched the GUID number of an individual trading child pornography in Florida just a few months prior is evidence that is proximate to the date of the charged offense, is necessary to explain how Defendant was identified as the primary suspect, and is related to the inception of the charges in the indictment. The testimony evidence is thus properly admitted as background or identification evidence, and the Government's amended motion will be granted.

Accordingly, it is **ORDERED** that the Government's amended motion to include testimony evidence of other acts inextricably intertwined with the charged acts (ECF No. 36) is **GRANTED**.

s/Thomas L. Ludington
THOMAS L. LUDINGTON
United States District Judge

Dated: May 8, 2012

PROOF OF SERVICE

The undersigned certifies that a copy of the foregoing order was served upon each attorney of record herein by electronic means or first class U.S. mail on May 8, 2012.

s/Tracy A. Jacobs
TRACY A. JACOBS